Title: On an equation of Sophie Germain

Author: Radosław Łukasik, Justyna Sikorska, Tomasz Szostok

Citation style: Łukasik Radosław, Sikorska Justyna, Szostok Tomasz. (2018). On an equation of Sophie Germain. "Results in Mathematics" (Vol. 73, no. 2 (2018), art. no. 60), doi 10.1007/s00025-018-0820-y

Results Math (2018) 73:60

1422-6383/18/020001-7
published online April 6, 2018
https://doi.org/10.1007/s00025-018-0820-y

Results in Mathematics

On an Equation of Sophie Germain

Radosław Łukasik, Justyna Sikorska, and Tomasz Szostok

Abstract. We deal with the following functional equation

$$f(x)^2 + 4f(y)^2 = \big(f(x+y) + f(y)\big)\big(f(x-y) + f(y)\big)$$

which is motivated by the well known Sophie Germain identity. Some connections as well as some differences between this equation and the quadratic functional equation

$$f(x+y) + f(x-y) = 2f(x) + 2f(y)$$

are exhibited. In particular, the solutions of the quadratic functional equation are expressed in the language of biadditive and symmetric functions, while the solutions of the Sophie Germain functional equation are of the form: the square of an additive function multiplied by some constant. Our main theorem is valid for functions taking values in a unique factorization domain. We present also an example which shows that our main result does not hold in each integral domain.

Mathematics Subject Classification. 39B05.

Keywords. Sophie Germain identity, quadratic functional equation, biadditive and symmetric functions, functional equations on integral domains.

1. Introduction

We deal with a functional equation motivated by the identity

$$a^4 + 4b^4 = \big((a+b)^2 + b^2\big)\big((a-b)^2 + b^2\big) \tag{1}$$

which is attributed to Sophie Germain. In fact, she mentioned only the identities

$$p^2 + 4 = (p^2 - 2)^2 + 4p^2$$

(which, in view of Fermat's two squares theorem, implies that no number of the form p^2+4 is prime) and

$$p^4+q^4=(p^2-q^2)^2+2p^2q^2=(p^2+q^2)^2-2p^2q^2,$$

for details see [4,6]. Although (1) is very easy to check, it is extremely useful in solving number theory problems. It is also a common tool for contests problems like: show that the number $5^{444}+4^{555}$ is not prime or calculate the sum of the series $\sum_{n=1}^{\infty}\frac{k}{4k^4+1}$, for details see for example [7].

Inspired by the identity (1), we consider the following functional equation

$$f(x)^2+4f(y)^2=\big(f(x+y)+f(y)\big)\big(f(x-y)+f(y)\big). \tag{2}$$

It is immediately seen that the function $f(x)=cx^2$ is a solution of (2). We ask if there are any solutions of (2) other than $f(x)=cx^2$. Since we do not want to assume any regularity conditions of the functions in question, the first guess is that (2) may be equivalent to the equation of a quadratic function

$$f(x+y)+f(x-y)=2f(x)+2f(y). \tag{3}$$

Surprisingly, it will turn out that only some solutions of the quadratic functional equation (3) satisfy (2). It is a rare behavior in the world of functional equations. Dealing with functional equations it is more common that either an equation preserves all solutions of the linear equation it is connected with or it forces the continuity of its solutions (like Aczél equation

$$F(y)-F(x)=(y-x)f\left(\frac{x+y}{2}\right)$$

does, see [1]).

2. Main Results

Assume that $(G,+)$ is an abelian group, R is an integral domain.

Lemma 1. *Let* $\operatorname{char} R\neq 2$. *If* $f\colon G\to R$ *satisfies* (2) *for all* $x,y\in G$ *then it is even.*

Proof. It is easy to see that $f(0)=0$. Put $x:=0$ into (2) in order to obtain

$$\begin{aligned}4f(y)^2&=2f(y)\big(f(-y)+f(y)\big),\quad y\in G,\\ 2f(y)\big(f(-y)-f(y)\big)&=0,\quad y\in G,\end{aligned}$$

whence

$$f(y)^2=f(y)f(-y),\quad y\in G. \tag{4}$$

Surely, we also have $f(-y)^2=f(y)f(-y)$ for all $y\in G$. Consequently, $f(y)^2=f(-y)^2$ for all $y\in G$ and $f(y)=0$ if and only if $f(-y)=0$. Therefore, if $f(y)\neq 0$ then by (4), $f(y)=f(-y)$, and finally, f is even. □

The following example shows that the assumption that R is an integral domain is essential.

Example 1. Let $f\colon \mathbb{Z}_4 \to \mathbb{Z}_4$ is given by

$$f(x) = \begin{cases} x & \text{if } x \neq 0 \\ 2 & \text{if } x = 0. \end{cases}$$

Then f satisfies (2) and it is not even.

Lemma 2. *If $f\colon G \to R$ satisfies (2) for all $x, y \in G$ then $f(2x) = 4f(x)$ for all $x \in G$.*

Proof. Observe first that if $f(x) = 0$ for some $x \in G$ then $f(2x) = 0$. Indeed, assume $f(x_0) = 0$. It is enough to put $x := 2x_0$ and $y := x_0$ into (2) in order to get the assertion.

Put now $y := x$ in (2). Then $5f(x)^2 = \big(f(2x) + f(x)\big)f(x)$ for all $x \in G$, which gives

$$f(x)\big(f(2x) - 4f(x)\big) = 0, \quad x \in G,$$

and completes the proof. □

Theorem 1. *Let* $\operatorname{char} R \neq 2$. *If $f\colon G \to R$ satisfies (2) for all $x, y \in G$ then it is quadratic, i.e., it satisfies equation $f(x+y) + f(x-y) = 2f(x) + 2f(y)$ for all $x, y \in G$.*

Proof. By (2), we have

$$f(x)^2 + 3f(y)^2 = f(x+y)f(x-y) + f(y)\big(f(x+y) + f(x-y)\big), \quad x, y \in G. \tag{5}$$

Interchanging the roles of x and y and using Lemma 1 (the evenness of f) we obtain

$$f(y)^2 + 3f(x)^2 = f(x+y)f(x-y) + f(x)\big(f(x+y) + f(x-y)\big), \quad x, y \in G. \tag{6}$$

After subtracting Eq. (5) from (6) side by side we get

$$2f(x)^2 - 2f(y)^2 = \big(f(x) - f(y)\big)\big(f(x+y) + f(x-y)\big), \quad x, y \in G,$$

that is,

$$\big(f(x) - f(y)\big)\big(2f(x) + 2f(y) - f(x+y) - f(x-y)\big) = 0, \quad x, y \in G. \tag{7}$$

Substitute now $x+y$ and $x-y$ in the place of x and y, respectively, first in (2) and then in (7). By Lemma 2, we have

$$f(x+y)^2 + 4f(x-y)^2 = \big(4f(x) + f(x-y)\big)\big(4f(y) + f(x-y)\big), \quad x, y \in G \tag{8}$$

and

$$\big(f(x+y)-f(x-y)\big)\big(f(x+y)+f(x-y)-2f(x)-2f(y)\big)=0,\quad x,y\in G. \tag{9}$$

Suppose that for some $x,y\in R$ we have $f(x)=f(y)$ and $f(x+y)=f(x-y)$. Then by (2),

$$5f(x)^2=\big(f(x+y)+f(x)\big)^2, \tag{10}$$

and by (8),

$$5f(x+y)^2=\big(4f(x)+f(x+y)\big)^2. \tag{11}$$

From (10) and (11), it follows that $4f(x)f(x+y)=0$ which in turn gives $f(x)=f(x+y)=0$, and consequently, $f(x+y)+f(x-y)=2f(x)+2f(y)$.

Our assertion is now derived from (7) and (9). □

Remark 1. It is enough to consider the function $f:\mathbb{Z}_9\to\mathbb{Z}_9$ given by $f(x)=3$, $x\in\mathbb{Z}_9$, to see that the assumption that R is an integral domain is essential in Theorem 1.

Theorem 2. *Let* $\operatorname{char}R\neq 2$, $f\colon G\to R$. *Then* f *satisfies* (2) *if and only if there exists a unique biadditive and symmetric function* $A\colon G^2\to R$ *satisfying*

$$A(x,x)A(y,y)=A(x,y)^2,\quad x,y\in G \tag{12}$$

and such that $4f(x)=A(x,x)$ *for all* $x\in G$.

Proof. Assume that $4f(x)=A(x,x)$ for all $x\in G$, where $A\colon G^2\to R$ is a biadditive and symmetric function satisfying (12). Then we have

$$\begin{aligned}
&16\big(f(x+y)+f(y)\big)\big(f(x-y)+f(y)\big)\\
&\quad=\big(A(x+y,x+y)+A(y,y)\big)\big(A(x-y,x-y)+A(y,y)\big)\\
&\quad=\big(A(x,x)+2A(y,y)+2A(x,y)\big)\big(A(x,x)+2A(y,y)-2A(x,y)\big)\\
&\quad=\big(A(x,x)+2A(y,y)\big)^2-4A(x,y)^2\\
&\quad=A(x,x)^2+4A(y,y)^2+4A(x,x)A(y,y)-4A(x,y)^2\\
&\quad=16f(x)^2+64f(y)^2,\ x,y\in G,
\end{aligned}$$

which shows Eq. (2).

For the converse, by Theorem 1, function f is quadratic and by [3] (see also [2]) there exists a biadditive and symmetric function $A\colon G^2\to R$ such that $4f(x)=A(x,x)$ for all $x\in G$ (it is enough to define $A(x,y):=f(x+y)-f(x-y)$ for all $x,y\in G$ and to prove (see [3]) its symmetry, additivity with respect to the first variable and the uniqueness). Substituting the

form of f into (2) we obtain

$$\begin{aligned}0 &= 16\big(f(x+y)+f(y)\big)\big(f(x-y)+f(y)\big) - 16f(x)^2 - 64f(y)^2\\ &= \big(A(x+y,x+y)+A(y,y)\big)\big(A(x-y,x-y)+A(y,y)\big)\\ &\quad - A(x,x)^2 - 4A(y,y)^2\\ &= \big(A(x,x)+2A(y,y)+2A(x,y)\big)\big(A(x,x)+2A(y,y)-2A(x,y)\big)\\ &\quad - A(x,x)^2 - 4A(y,y)^2\\ &= \big(A(x,x)+2A(y,y)\big)^2 - 4A(x,y)^2 - A(x,x)^2 - 4A(y,y)^2\\ &= 4A(x,x)A(y,y) - 4A(x,y)^2,\ x,y\in G,\end{aligned}$$

which shows condition (12). □

Theorem 3. *Let R be a unique factorization domain with* $\operatorname{char} R \neq 2$. *Function $f\colon G\to R$ satisfies (2) if and only if there exist an additive function $a\colon G\to R$ and a constant $\gamma\in R$ such that $f=\gamma a^2$.*

Proof. Assume that f satisfies (2). In view of Theorem 2 there exists a bi-additive and symmetric function $A\colon G^2\to R$ satisfying (12). If $A(z,z)=0$ for all $z\in G$, then $f=0$. Assume that $A(z_0,z_0)\neq 0$ for some $z_0\in G$. Since $A(z_0,z_0)=4f(z_0)$, then there exist pairwise different prime elements $p_1,\dots,p_k,q_1,\dots,q_l$ of R, $n_1,\dots,n_k,m_1,\dots,m_l\in\mathbb{N}$, and a unit $u\in R$ such that

$$A(z_0,z_0) = 4u\cdot p_1^{2n_1}\cdot\ldots\cdot p_k^{2n_k}\cdot q_1^{2m_1-1}\cdot\ldots\cdot q_l^{2m_l-1}.$$

Let $\gamma = u^{-1}\cdot q_1\cdot\ldots\cdot q_l$, $\alpha = 4p_1^{n_1}\cdot\ldots\cdot p_k^{n_k}\cdot q_1^{m_1}\cdot\ldots\cdot q_l^{m_l}$. For every $x\in G$ there exist prime elements $d_1,\dots,d_j$ of R different from $p_1,\dots,p_k,q_1,\dots,q_l$, numbers $s_1,\dots,s_k,t_1,\dots,t_l\in\mathbb{N}\cup\{0\}$ and a unit $v\in R$ such that

$$A(x,x) = 4v\cdot p_1^{s_1}\cdot\ldots\cdot p_k^{s_k}\cdot q_1^{t_1}\cdot\ldots\cdot q_l^{t_l}\cdot d_1\cdot\ldots\cdot d_j.$$

Using (12) we obtain

$$A(x,z_0)^2 = 16uv\cdot p_1^{2n_1+s_1}\cdot\ldots\cdot p_k^{2n_k+s_k}\cdot q_1^{2m_1-1+t_1}\cdot\ldots\cdot q_l^{2m_l-1+t_l}\cdot d_1\cdot\ldots\cdot d_j.$$

Hence, $s_1,\dots,s_k$ are even, $t_1,\dots,t_l$ are odd and

$$A(x,z_0) = 4w\cdot p_1^{n_1+\frac{s_1}{2}}\cdot\ldots\cdot p_k^{n_k+\frac{s_k}{2}}\cdot q_1^{m_1+\frac{t_1-1}{2}}\cdot\ldots\cdot q_l^{m_l+\frac{t_l-1}{2}}\cdot r_1\cdot\ldots\cdot r_i$$

for some prime elements $r_1,\dots,r_i$ of R different from $p_1,\dots,p_k,q_1,\dots,q_l$ and a unit $w\in R$. Now we have

$$\frac{A(x,z_0)}{\alpha} = w\cdot p_1^{\frac{s_1}{2}}\cdot\ldots\cdot p_k^{\frac{s_k}{2}}\cdot q_1^{\frac{t_1-1}{2}}\cdot\ldots\cdot q_l^{\frac{t_l-1}{2}}\cdot r_1\cdot\ldots\cdot r_i\in R.$$

Define $a\colon G\to R$ by the formula $a(x)=\frac{A(x,z_0)}{\alpha}$ for $x\in G$. It is obvious that a is additive. We have also

$$4\alpha^2 f(x) = \alpha^2 A(x,x) = 4\gamma A(z_0,z_0)A(x,x) = 4\gamma A(x,z_0)^2 = 4\gamma\alpha^2 a(x)^2,$$

for all $x\in G$, which shows that $f=\gamma a^2$.

Now assume that $f = \gamma a^2$ for some additive function $a\colon G \to R$ and a constant $\gamma \in R$. Then we define $A\colon G^2 \to R$ by the formula

$$A(x,y) = 4\gamma a(x)a(y),\ x,y \in G.$$

It is obvious that A is biadditive, symmetric and $A(x,x) = 4f(x)$ for $x \in G$. We have also

$$A(x,y)^2 = 16\gamma a(x)^2 a(y)^2 = A(x,x)A(y,y),\ x,y \in G,$$

so A satisfies (12) and in view of Theorem 2, f satisfies (2). □

Corollary 1. *Let $f\colon \mathbb{Z} \to \mathbb{Z}$. Then f satisfies (2) if and only if there exists $\gamma \in \mathbb{Z}$ such that $f(x) = \gamma x^2$ for all $x \in \mathbb{Z}$.*

Proof. In view of Theorem 3, f satisfies (2) if and only if there exist $\beta \in \mathbb{Z}$ and an additive function $a\colon \mathbb{Z} \to \mathbb{Z}$ such that $f = \beta a^2$. Since for the additive map a we have $a(m) = ma(1)$ for $m \in \mathbb{Z}$ then taking $\gamma = \beta a(1)^2$ we derive that f satisfies (2) if and only if there exists $\gamma \in \mathbb{Z}$ such that $f(x) = \gamma x^2$. □

The following example shows that Theorem 3 may not hold in integral domains that are not unique factorization domains.

Example 2. Let $R = \langle 1, X^3, X^4, X^5, \ldots\rangle$ be a subring of $\mathbb{Q}[X]$. Define $A\colon R^2 \to R$ by

$$\begin{aligned} &A\big(a_0 + a_3X^3 + \cdots + a_nX^n, b_0 + b_3X^3 + \cdots + b_mX^m\big)\\ &\quad = a_0b_0X^3 + \big(a_0b_3 + a_3b_0\big)X^4 + a_3b_3X^5 \end{aligned}$$

for all $a_0, a_3, \ldots, a_n, b_0, b_3, \ldots, b_m \in \mathbb{Q}$, $m, n \geq 3$. It is easy to see that A is biadditive and symmetric. We have also

$$\begin{aligned} &A(a_0+a_3X^3 + \cdots + a_nX^n, b_0 + b_3X^3 + \cdots + b_mX^m)^2\\ &\quad = \big(a_0b_0X^3 + \big(a_0b_3 + a_3b_0\big)X^4 + a_3b_3X^5\big)^2\\ &\quad = a_0^2b_0^2X^6 + 2\big(a_0^2b_0b_3 + a_0a_3b_0^2\big)X^7 + (4a_0a_3b_0b_3 + a_0^2b_3^2 + a_3^2b_0^2)X^8\\ &\qquad + 2\big(a_0a_3b_3^2 + a_3^2b_0b_3\big)X^9 + a_3^2b_3^2X^{10}\\ &\quad = \big(a_0^2X^3 + 2a_0a_3X^4 + a_3^2X^5\big)\big(b_0^2X^3 + 2b_0b_3X^4 + b_3^2X^5\big)\\ &\quad = A\big(a_0 + a_3X^3 + \cdots + a_nX^n, a_0 + a_3X^3 + \cdots + a_nX^n\big)A\big(b_0 + b_3X^3\\ &\qquad + b_mX^m, b_0 + b_3X^3 + \cdots + b_mX^m\big), \end{aligned}$$

so, A satisfies (12).

Suppose that there exist an additive map $a\colon R \to R$ and $\gamma \in R$ such that $A(x,x) = \gamma a(x)^2$ for $x \in R$. We have $\gamma a(1)^2 = A(1,1) = X^3$, so $a(1) = q$ for some $0 \neq q \in \mathbb{Q}$ and $\gamma = \frac{1}{q^2}X^3$. We observe that $\gamma a(X^3)^2 = A(X^3, X^3) = X^5$, whence, $a(X^3)^2 = q^2X^2 \notin R$, which is a contradiction.

References

[1] Aczél, J.: A mean value property of the derivative of quadratic polynomials—without mean values and derivatives. Math. Mag. **58**, 42–45 (1985)

[2] Aczél, J.: The general solution of two functional equations by reduction to functions additive in two variables and with aid of Hamel-bases. Glasnik Mat. Fiz. Astronom. Društvo Mat. Fiz. Hrvatske (2) **20**, 65–73 (1965)

[3] Aczél, J., Dhombres, J.: Functional Equations in Several Variables. Encyclopedia of Mathematics and Its Applications, vol. 31. Cambridge University Press, Cambridge (1989)

[4] Dickson, L.E.: History of the Theory of Numbers, vol. 1. Chelsea Publishing Company, New York (1952)

[5] Engel, A.: Problem-Solving Strategies. Springer, New York (1998)

[6] http://www.theoremoftheday.org/Binomial/GermainId/TotDGermainIdentity.pdf

[7] https://topologicalmusings.wordpress.com/2008/02/20/sophie-germain-identity/

Radosław Łukasik, Justyna Sikorska and Tomasz Szostok
Institute of Mathematics
University of Silesia
ul. Bankowa 14
40-007 Katowice
Poland
e-mail: rlukasik@math.us.edu.pl

Justyna Sikorska
e-mail: justyna.sikorska@us.edu.pl

Tomasz Szostok
e-mail: tszostok@math.us.edu.pl

Received: December 22, 2017.
Accepted: March 28, 2018.